Claims

[c1] 1.A system comprising:

a computer peripheral, detecting information about a current surrounding of the computer; and

a computer, running a routine which allows a user to identify themselves to the computer, and controls access to the computer based on said identify and said current surrounding.

[c2] 2.A system as in claim 1, wherein said computer determines a first surrounding at a time of user identification, and maintains the computer unlocked while the computer is in said first surrounding, and causes the computer to lock when the computer is detected to vary from said first surrounding by a predetermined amount.

[c3] 3.A system as in claim 2, wherein said surrounding is a physical location of the computer, as detected by an automatic position location device.

[c4] 4.A system as in claim 2, wherein said surrounding includes a view that is seen by the computer.

[c5] 5.A system as in claim 4, wherein said view includes an image of a user.

[c6] 6.A system as in claim 2, further comprising a failure processing routine, which processes failures in login by increasing security for each of a plurality of times when a login fails.

[c7] 7.The system as in claim 6, further comprising increasing a security of the computer when a user powers down the computer in response to being prompted to identify themselves.

[c8] 8.A method, comprising:

carrying out a first security operation which allows a user to obtain access to resources of the computer;

determining surroundings information, including first surroundings information associated with said first security operation, and second surroundings

information at times subsequent to said first surroundings information; and allowing continued access to resources of the computer only so long as said second surroundings information does not differ from said first surroundings information by more than a specified threshold, and if said second surroundings information differs from said first surroundings information by more than said specified threshold, then requiring a new security operation to obtain said access to said resources.

[c9] 9.A method as in claim 8, wherein said surroundings information is information indicative of a physical location of the computer, and said determining comprises using an automatic position determining device to determine said position.

[c10] 10.A method as in claim 8, wherein said surroundings information is information indicative of an image of a proximity of said computer, and said determining comprises using a camera to determine said image.

[c11] 11.A method as in claim 9, further comprising determining a difference between said first and second surroundings information, determining a distance between the physical locations indicated by said first and second surroundings information, determining if said distance is greater than a predetermined threshold, and allowing said continued access only when said distance is not greater than said predetermined threshold.

[c12] 12.A method as in claim 10, further comprising determining a difference between a first image representing said first surroundings information, and a second image representing said second surroundings information, using automated machine vision techniques.

[c13] 13.A method as in claim 8, wherein said first security operation comprises determining whether a user has successfully responded to a request for user-security information, and for each of the plurality of times that the user does not successfully respond to said request for user-security information, increasing an aspect of security.

[c14] 14. A method as in claim 13, wherein said increased aspect of security includes entry of secret personal information.

[c15] 15.A method, comprising:
detecting an attempt to obtain access to computer resources and maintaining a number of times that said attempt has been made; and
for each of said plurality of attempts, increasing a security of said computer resources.

[c16] 16.A method as in claim 15, wherein said increasing a security comprises encrypting specified files, wherein additional files are encrypted each time that an attempt to obtain access is made.

[c17] 17.A method as in claim 15, wherein said increasing a security comprises requiring additional information prior to granting said access.

[c18] 18. A method as in claim 8, wherein said determining comprises triangulating to determine a position.

[c19] 19. A system comprising:
a computer, running a routine which allows a user to identify themselves to the computer, and
a file access detecting part, detecting access to a specified higher security file on said computer, and requiring a user to re-identify themselves to the computer upon said detecting said access to said specified higher security file, but not requiring the user to re identify themselves to the computer upon detecting access to files other then said specified higher security files.

[c20] 20. A system as in claim 19, wherein said higher security files are manually marked as high security files.

[c21] 21. A system as in claim 19, wherein said file access detecting part automatically detects specified words in said files, and automatically determines files including said specified words as being said higher security files.